UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT
EASTERN DIVISION OF OHIO

In the Matter of the Search of:	)	**No.** 2:24-mj-400
	)	
The Snapchat accounts, including all information and Content, associated with the identifiers Listed in Attachment A and referred to as SUBJECT ACCOUNTS, that are stored at the Premises Controlled by Snapchat, Inc.	)	**Magistrate Judge**
	)	
	)	**UNDER SEAL**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Amanda North (Your Affiant), a Special Agent with the Ohio Bureau of Criminal Investigation (BCI) and assigned as a Task Force Officer (TFO) for the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

EDUCATION TRAINING AND EXPERIENCE

1. I am a Special Agent (SA) with BCI, since 2022, and have been in the Special Victims Unit since 2013, where I was previously a Criminal Investigator. I have been a TFO at the FBI Columbus Resident Agency since early 2023. I am primarily responsible for investigating child sexual exploitation and internet crimes, as well as hands on offenses of abuse involving juveniles and the elderly.
2. During my career as a Criminal Investigator, I have received more than one hundred hours of training in internet investigations, to include Peer to Peer software. I was assigned full-time to the Franklin County Internet Crimes Against Children Task Force (ICAC), from January of 2016 through my promotion to SA in May of 2022. I was also a TFO for Homeland Security from 2018 until the end of 2021, when I was designated to be assigned to the FBI VCAC Unit. I have participated in various investigations of child exploitation and have executed numerous search warrants, interviews and arrests that resulted in conviction. As part of my duties as a TFO, I investigate criminal violations relating to child exploitation and child pornography

violations, including the illegal production, distribution, transmission, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A.

3. As a TFO with the FBI, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

PURPOSE OF THE AFFIDAVIT

4. I make this affidavit in support of an application for a search warrant for information associated with certain Snapchat Screen/Username that is stored at premises owned, maintained, controlled, or operated by Controlled by Snap, Inc. ("Snapchat"), a social networking company headquartered at 2772 Donald Douglas Loop North, in Santa Monica, California**.** The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Snapchat to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the Screen/Username "Zackadkins1234" and "Zackadkins21" hereinafter the **SUBJECT ACCOUNTS**.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers, agents, and witnesses. I have set forth only the facts necessary to establish probable cause for a search warrant for the content of the **SUBJECT ACCOUNTS**. I have not omitted any facts that would negate probable cause.

6. The **SUBJECT ACCOUNTS** to be searched is more particularly described in Attachment A, for items specified in Attachment B, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2252A- sexual exploitation of a minor, advertisement of/for and distribution, transmission, receipt, and/or possession of child pornography. I am requesting authority to search the entire content of the **SUBJECT ACCOUNTS**, wherein the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

APPLICABLE STATUTES AND DEFINITIONS

7. Title 18, United States Code, Section 2251(a), makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any

visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or that the visual depiction was produced or transmitted using materials that have been mailed, shipped or transported in or affecting interstate or foreign commerce, or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce. Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.

8. Title 18, United States Code, Section 2251(d)(1)(A) makes it a federal crime for any person to make, print, publish, or cause to be made, printed or published, any notice or advertisement that seeks or offers to receive, exchange, buy, produce, display, distribute or reproduce, any visual depiction involving the use of a minor engaging in sexually explicit conduct, if such person knows or has reason to know that either the notice or advertisement will be transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail; or that the notice or advertisement actually was transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail.
9. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.
10. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly transport, receive, or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a crime to possess or access with intent to view any material that contains an image of child pornography that has been

mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

11. As it is used in 18 U.S.C. §§ 2251 and 2252, the term "sexually explicit conduct" is defined in 18 U.S.C. § 2256(2)(A) as actual or simulated: sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.
12. As it is used in 18 U.S.C. § 2252A(a)(2), the term "child pornography" [1] is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or in indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
13. The term "sexually explicit conduct" has the same meaning in § 2252A as in § 2252, except that for the definition of child pornography contained in § 2256(8)(B), "sexually explicit conduct" also has the meaning contained in § 2256(2)(B): (a) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (b) graphic or lascivious simulated (i) bestiality, (ii) masturbation, or (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.
14. The term "minor", as used herein, is defined pursuant to Title 18, United States Code, Section 2256(1) as "any person under the age of eighteen years."
15. The term "graphic," as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean "that a viewer can

[1] The term child pornography is used throughout this affidavit. All references to this term in this affidavit and Attachments A and B hereto, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. §§ 2251 and 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted.

16. The term "visual depiction," as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to "include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image."
17. The term "computer" is defined in Title 18 U.S.C. § 1030(e)(1) and 2256(6) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
18. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
19. "Cellular telephone" or "cell phone" means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving videos; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and

downloading information from the Internet. Wireless telephones may include geographic information indicating where the cell phone was at particular times.

20. "Internet Service Providers" (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
21. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.
22. As it is used throughout this affidavit and all attachments hereto, the term "storage media" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

BACKGROUND INFORMATION REGARDING SOCIAL MEDIA AND SNAP

23. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and conversations with other officers, I know the following:
24. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. Many individual computer users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information,

account application information, Internet Protocol addresses and other information both in computer data format and in written record format.

25. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

26. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications. Mobile applications, also referred to as "apps," are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game. Examples of such "apps" include LiveMe, Kik messenger service, Snapchat, Meet24, and Instagram.

27. According to the Snap Law Enforcement Guide, "Snapchat is a mobile application made by Snap Inc. ("Snap") and available through the iPhone App Store and Google Play Store. The Snapchat app provides users a way to share moments with photos, videos, and chats." Snapchat's differentiating feature from other communications applications is that a sender is able to set a variable amount of time the message is viewable by the receiver. This time can be between one and ten seconds. At the expiration of time, the message is deleted from Snapchat's servers. Similarly, the message disappears from the user's devices. If the receiver of a Snapchat message does not access the application on their device, the message remains undelivered. Snap's services are designed to store unopened snaps for 30 days. After 30 days the messages are deleted from Snap's servers.

28. Snapchat users have the following abilities:

    A. Snaps: photos or videos taken using his or her phone's camera (or the Snapchat app's camera), which may be shared directly with the user's friends, or in a Story (explained below), or Chat. Snaps can also be sent from the saved

pictures/videos in the gallery of the device. Unless the sender or recipient opts to save the photo or video, the message will be deleted from their devices (after the content is sent in the case of the sender and after it is opened in the case of the recipient). Users are able to save a photo or video they've taken locally to their device or to Memories, which is Snapchat's cloud-storage service.

B. Stories: A user can add photos or videos (Snaps) to their "Story." A Story is a collection of Snaps (*i.e.*, photos or videos) displayed in chronological order. Users can manage their privacy settings so that their Story can be viewed by all Snapchatters, their friends, or a custom audience. A user can also submit their Snaps to Snap's crowd-sourced service "Our Story," which enables their Snaps to be viewed by all Snapchatters in search and Snap Map. Snap's servers are designed to automatically delete a Snap in a user's Story 24 hours after the user posts the Snap, but the user may delete part or all of the Story earlier. Submissions to Our Story may be saved for longer periods of time.

C. Memories: Snapchat's cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone's photo gallery in Memories. Content saved in Memories is backed up by Snap and may remain in Memories until deleted by the user. Users may encrypt their content in Memories (called "My Eyes Only"), in which case content is not accessible to Snap and cannot be decrypted by Snap.

D. Chat: A user can also type messages, send photos (Snaps), audio notes, and video notes to friends within the Snapchat app using the Chat feature. Snap's servers are designed to automatically delete one-to-one chats once the recipient has opened the message and both the sender and recipient have left the chat screen, depending on the user's chat settings. Within the Snapchat app itself, a user can opt to save part of the Chat by tapping on the message that they want to keep. The user can clear the message by tapping it again. This will result in it being deleted from Snap's services. Users can also delete chats that they have sent to a recipient before the recipient has opened the chat or after the recipient has saved the chat. Users can also chat in groups. Chats sent in groups are deleted after 24 hours whether they are opened or not.

E. Location Data: If a user has device-level location services turned on and has opted into location services on Snapchat, Snap will collect location data at various points during the user's use of Snapchat, and retention periods for location data vary depending on the purpose of the collection. Users have some control over the deletion of their location data in the app settings.

29. Information that Snapchat possesses and maintains:

A. Personal Identifying Information: When a user creates an account, they make a unique Snapchat username. This is the name visible to other Snapchat users. A user also enters a data of birth. This is supposed to prevent anyone under the age of 13 from using Snapchat. An email address is required to register a Snapchat account. A new user also has to provide a mobile phone number. This phone number is verified during the registration process. Snapchat sends an activation code that must be entered before proceeding with the registration step. However, a user may elect to bypass entering a phone number so one may not always be present in the user's account. Snapchat also retains the account creation date.

B. Usage Information: While a Snapchat message may disappear, the record of who sent it and when still exists. Snapchat records and retains log files and information that is roughly analogous to the call detail records maintained by telecommunications companies. This includes the date, time, sender, and recipient of a snap. Additionally, Snapchat stores the number of messages exchanged, which users they communicate with the most, message status including if and when the message was opened, and whether the receiver used the native screen capture function of their device to take a picture of the snap before it disappeared.

C. Device Information: Snapchat stores device information such as the model, operating system, operating system version, mobile device phone number, and mobile network information of devices used in conjunction with the service. They also collect unique device identifiers such as the Media Access Control (MAC) address and the International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of devices used to access Snapchat.

D. Device Phonebook and Photos: If a user consents, Snapchat can access from their device's electronic phonebook or contacts list and images.

E. Location Data: may be available for a Snapchat user who has turned on location services on their device and opted into location services in the app settings.

F. Message Content: Because Snap's servers are designed to automatically delete most user content, and because much of a user's content is encrypted, Snap often cannot retrieve user content except in very limited circumstances. For example, Memories content may be available until deleted by a user.

30. If a user has device-level location services turned on and has opted into location services on Snapchat, Snap will collect location data at various points during the user's use of Snapchat, and retention periods for location data vary depending on the purpose of the collection. Users have some control over the deletion of their location data in the app settings.

31. Therefore, the computers/servers of Snapchat are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Snapchat, such as account access information, transaction information, and other account information.

INVESTIGATION AND PROBABLE CAUSE

32. On or about May 9, 2024 an online tip was received by the FBI National Threat Operations Center (NTOC), regarding alleged sexual exploitation of minors via the application Snapchat. The report was submitted by an email address known to your affiant using IP address 76.34.127.13, which resolved to Marysville, Ohio 43040.

33. The reporting party, identified as Jane Doe, documented in the tip that the target was Zachary William Adkins (ADKINS), DOB 07/18/1996 and with associated phone number (614) 327-8557. Jane Doe reported that ADKINS had been "caught on multiple occasions sending sexual content to minors, to include pictures of his penis on the platform Snapchat and knew the females to have been between 14-16 years of age. He also lied and told them he is younger than his current age." Moreover, Jane Doe indicated in the tip that ADKINS was requesting nude content from minors.

34. On or about May 14, 2024, law enforcement contacted Jane Doe, to obtain additional information on the lead. Jane Doe provided two Snapchat accounts that were owned and utilized by ADKINS as zackadkins21 and zackadkins1234 (the **SUBJECT ACCOUNTS**).

35. Jane Doe stated that ADKINS has had at least four Snapchat accounts that he utilized to communicate with underage females, but that ADKINS current girlfriend had caught ADKINS sharing explicit content with the juveniles and made him delete some of the accounts. Jane Doe was unsure of any additional usernames or profiles that ADKINS may have.
36. Specifically, in 2022, Jane Doe saw a conversation on ADKINS' device, in which ADKINS was communicating with whom Doe believed to be a juvenile. Doe stated that the juvenile asked ADKINS why he was sending her nude images of himself if he had a wife.
37. Doe also alleged that ADKINS reached out to Doe's 14 year old cousin and attempted to engage in sexual conversation with the juvenile.
38. Both Doe and the current girlfriend have seen nude images of juveniles on ADKINS' devices, and confronted him. The juveniles were believed to be between 14 and 16 years of age.
39. Jane Doe further indicated that ADKINS has three underage children himself, and Jane Doe has concerns about them being around ADKINS.
40. Jane Doe advised that although ADKINS girlfriend is aware of the activities of ADKINS, she will not cooperate with law enforcement. However, up until the time in which law enforcement contacted Jane Doe, ADKINS girlfriend had been relaying to Jane Doe what she had observed on ADKINS' device. Jane Doe alleged that ADKINS girlfriend had been planning to leave ADKINS, but that ADKINS had promised to delete the accounts and cease the interactions with juveniles.
41. On or about May 15, 2024, law enforcement requested preservations on the two identified Snapchat accounts, prior to subpoenas being issued for subscriber information.
42. That same day, law enforcement searched the Internet Crimes Against Children Data Systems (ICAC IDS) site to identify any additional leads that included the identifiers of Zachary Adkins or the known Snapchat usernames. Two National Center for Missing and Exploited Children (NCEMC) CyberTipline reports were located - Report #100907964 and Report #100436470, which were both dated September of 2021. In the CyberTipline reports, the Electronic Service Provider Meta, specifically Facebook, indicated that a user identified as Zack Adkins, DOB of 07/18/1996, verified phone number of 614-327-8557, and verified email address of zadkins482@gmail.com had received child pornography files on Facebook.

43. On or about July 11, 2024, law enforcement reviewed the Snapchat responsive data for identifiers zackadkins21 and zackadkins1234. The zackadkins21 account, created on January 3, 2021 had a display name of "zack" and an associated phone number of 614-783-2244.
44. A subpoena issued to T-Mobile for 614-783-2244 indicated that the account was active from March 15, 2021 through December 3, 2023. No identifying information was included.
45. The zackadkins1234 account was created on October 13, 2017 and has a display name of "renesmee Daddy", which includes a reference to ADKINS daughter.
46. Based on the information that has been gathered to date by your affiant, your affiant has reason to believe that the **SUBJECT ACCOUNTS** have sought out, produced, distributed and/or received child pornography. Therefore, it is likely that the **SUBJECT ACCOUNT** contains items which constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2252A- sexual exploitation of a minor, advertisement of/for and distribution, transmission, receipt, and/or possession of child pornography.

COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

47. Based on my own knowledge, experience, and training in online child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals who have a sexual interest in minors and/or seek to sexually exploit minors via online communications:
    A. Those who have a sexual interest in minors, may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from discussions of or literature describing such activity.
    B. Those who have a sexual interest in children and/or seek to sexually exploit minors via online communications may collect sexually explicit or suggestive materials in a variety of media. These materials are frequently used for the sexual arousal and gratification of the individual. Further, they may use these

materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

C. Individuals who have a sexual interest in children have been found to: download, view, then delete child pornography on a cyclical and repetitive basis; view child pornography without downloading or saving it; or save child pornography materials to cloud storage.

D. Those who have a sexual interest in minors may correspond online with and/or meet others to share information about how to find child victims, exchange stories about their sexual exploits with children, and/or exchange child pornography materials; and tend to conceal and maintain in a safe, secure and private environment such correspondence as they do any sexually explicit material related to their illicit sexual interest.

E. When communications relating to a sexual interest in children, and/or child pornography files are stored on or accessed by computers and related digital media, forensic evidence of the accessing, downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such files have been deleted from the computers or digital media.

48. Based upon the conduct of individuals who have a sexual interest in children and/or seek to sexually exploit minors via online applications and platforms, as set forth in the above paragraphs, there is probable cause to believe that evidence of the offenses of sexual exploitation of a minor, advertisement of/for, receipt and distribution and possession of child pornography is currently located on the **SUBJECT ACCOUNTS.**

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZE

49. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(l)(A) and 2703(c)(1)(A), by using the warrant to require Snapchat, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment.

CONCLUSION

50. Based on the forgoing factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. §§ 2251, 2252, and 2252A- sexual exploitation of a minor, advertisement of/for and distribution, transmission, receipt, and/or possession of child pornography is located in the content of the **SUBJECT ACCOUNTS**. Your affiant respectfully requests that the Court issue a search warrant authorizing the search of the **SUBJECT ACCOUNTS** described in Attachment A, and the seizure of the items described in Attachment B. Your affiant respectfully requests that the Court issue a search warrant authorizing the search of the **SUBJECT ACCOUNTS** described in Attachment A, and the seizure of the items described in Attachment B.

51. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Furthermore, because the warrant will be served on Snap, Inc., who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Amanda North Digitally signed by Amanda North DN: CN=Amanda North Reason: I am the author of this document Location: Date: 2024.08.14 11:21:12-04'00' Foxit PDF Editor Version: 13.1.2

Amanda North
TFO
Federal Bureau of Investigation

Sworn to and subscribed before me this 14th day of August, 2024.

Kimberly A. Johnson
United States Magistrate Judge